AUDITOR OF PUBLIC ACCOUNTS

February 5, 2003

# AUDITOR ALERT

Auditor of Public Accounts warns state and local government agencies to take all necessary precautions to protect proprietary and personal, confidential information residing on computer systems taken out of service.

The disposition of government computers requires that their files first be sanitized, eliminating all proprietary and personal, confidential information through destructive overwriting. Our recent forensic analysis of eight surplused computers chosen at random from the inventory of property earmarked for disposition by the Division of Surplus Properties identified confidential data. These data were in clear text, unprotected, and easily accessed. Preliminary discoveries include email, interagency correspondence and memoranda, financial accounting transactions, personal financial data, and HIV/AIDS data.

Deleting data or reformatting disks is not sufficient.

The State Auditor recommends using a floppy-based, bootable operating system such as Linux to destructively overwrite the partition table, logical partitions, and extended partitions of each hard disk, using dd, srm, and fdisk. These tools are available on the Internet and included in the Linux Operating System.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires government agencies to adequately secure confidential medical data, and imposes severe civil and criminal penalties for noncompliance, including heavy fines and/or imprisonment. Agencies must adhere to HIPAA's requirements.

Data security is the responsibility of the custodians of the data, and not the Division of Surplus Properties or subsequent recipients of the computers.